最近の素数判定アルゴリズム(数式処理における理論と応用の研究)

AUTHOR(S):

牧野, 潔夫

CITATION:

牧野, 潔夫. 最近の素数判定アルゴリズム(数式処理における理論と応用の研究). 数理解析研究所講究録 1993, 848: 58-73

ISSUE DATE:

1993-09

URL:

http://hdl.handle.net/2433/83661

数理解析研究所講究録
第848巻 1993年 58-73

最近の素数判定アルゴリズム

工学院大学　牧野 潔夫 (Isao MAKINO)

1. はじめに

計算の複雑さをを表わすために“計算量”という言葉がある。厳密な定義は長くなるのでここでは述べないが、簡単にいえば“計算(四則)を行う回数”である。ある問題を解決するために計算をするとき、その計算量が入力サイズ l の多項式以下のとき、計算量は多項式時間(または確定的多項式時間)であるといい、ある問題が多項式時間の計算量で計算する方法があるとき、その問題を(確定的)多項式時間計算可能問題という。計算量が l の指数関数になると l が大きくなれば殆ど計算不能であるので、ある問題が多項式時間計算可能であることは実際に計算するうえでは重要なことである。しかしある問題が多項式時間計算可能であるかどうかを判定するのは大変困難なことである。

更にある問題を解くとき、特定の選択肢の中から1つを任意に選ぶ必要があり、そのうちうまい選択をとると計算量が多項式時間になるもの(実際に計算を完了するまでうまい選択かどうかかはわからない)が選択肢全体の“$1/(l$ の多項式$)$”以上ある問題を確率的多項式計算時間可能問題ということにする。

以下の章では N が素数かどうかを判定する問題の計算量を考える。この問題では入力サイズは N の桁数であるから、多項式時間計算可能かどうかは、計算量が $\log(N)$ の多項式以下かどうかを調べればよい。近年得られた結果のうちここで紹介するものは次のものである。

ほとんど全ての素数は 確率的多項式時間 で素数と判定できる (Goldwasser-Kilian)。

素数判定は 確率的多項式時間計算可能問題 である (Adelman-Huang)。

一般 Riemann 予想を仮定すると、素数判定は 確定的多項式時間計算可能問題 である (Miller)。

以上の事実は近年の計算機の発展が数学に与えた影響により得られた結果のひとつであるといってもよい。またここでは扱わないが、最近の素数判定法に Gauss 和を用いた Adelman-Rumely-Pomerance の方法 [1]、Jacobi 和を用いた Cohen-Lenstra の方法 [5]、Bosma-van der Hulst の方法 [4] や楕円曲線を使った Moran 方法 [17] などがある。

この小論を書くにあたり、立教大学の木田祐司先生に参考文献の提供等多大の援助を受けました。記して感謝の意を表します。

2. 合成数判定

定理 1 (Fermat の小定理)

$$N\text{が素数で}\,\mathrm{GCD}(a,N)=1$$

ならば

$$a^{N-1}\equiv 1 \mathrm{mod} N \tag{1}$$

である。

また次の定理も成立する。

定理 2 (Euler の規準)

$$N\text{ が素数で }\mathrm{GCD}(a,N)=1$$

ならば

$$a^{\frac{N-1}{2}}\equiv\left(\frac{a}{N}\right)\mathrm{mod}N \tag{2}$$

が成り立つ。ただし $\left(\frac{a}{N}\right)$ は平方剰余記号である。

次の定理は単純だが強力である。

定理 3 (Miller)

$$N\text{ を素数とし }\mathrm{GCD}(a,N)=1,\ N-1=2^s d,\ \mathrm{GCD}(d,2)=1$$

とすると

$$a^d\equiv 1 \bmod N\ \text{又は}\ a^{2^k}\equiv -1 \bmod N\ \ (0\leq \exists k\leq s-1) \tag{3}$$

が成立する。

さてこれらの三定理の帰結 (1), (2), (3) は素数であることの十分条件ではあるが必要条件ではない。即ち N が条件 (1) (または (2), (3)) を満足しないならば N は素数でない即ち合成数とわかるが、N が (1) (または (2), (3)) を満足しても N が素数であるとはいえない。例えば 341 は $a=2$ のときの (1) を満足するが、$341=11\times 31$ であって素数ではない。このような合成数を a (今の例では 2) を底とする疑似素数 (pseudo prime with a base a), 記号で $psp(a)$ と表す。例えば $217=7\times 31$ は $psp(5)$ である。同様に Euler の定理の (2) を満たす合成数を a を底とする Euler 疑似素数 (Euler pseudo prime with a base a, 記号で $epsp(a)$) といい、定理 3 の場合は、(3) を満たす合成数を、a を底とする強疑似素数 (strong pseudo prime wit a base a, 記号で $spsp(a)$) という。$1105=13\times 17$ は $epsp(2)$ であり、$2047=23\times 89$ は $spsp(2)$ である。

N に対して a を十分たくさん動かしたとき、即ち $\mathrm{GCD}(a,N)=1, (1\leq a\leq N)$ なる a をすべて動かしたとき、これらの定理の条件 (1), (2), (3) を満足する数 N が素数になるかどうかを考える。残念ながら N が $1\leq a\leq N$ $(\mathrm{GCD}(a,N)=1)$ なる全ての a に対し条件 (1) を満たしても、即ち $\mathrm{GCD}(a,N)=1, 1\leq a\leq N, \mathrm{GCD}(a,N)=1$ なる全ての a に対し $a^{N-1}\equiv 1 \mathrm{mod} N$ であっても、N が素数であるとはいえない。このような合成数を Carmicae l 数という。一番小さい Carmicael 数は $561=3\times 11\times 17$ である。Carmicael

数が有限個か無限個かどうかという問題は未解決である。しかし条件 (2) に対してはつぎの事実が成立する。

命題 4 [21]
$\mathrm{GCD}(a,N)=1(1\leq a\leq N)$ なるすべての a に対し N が (2) を満たすならば N は素数である。

また

定理 5
任意の a $(\mathrm{GCD}(a,N)=1)$ に対し
N が (2) を満たすならば (1) を満たす。
N が (3) を満たすならば (2) を満たす。

この定理 5 と命題 4 により次の定理が成立する。

定理 6
$\mathrm{GCD}(a,N)=1(1\leq a\leq N)$ なるすべての a に対し N が (3) を満足するならば N は素数である。

故に N が合成数かどうかを調べるには $\mathrm{GCD}(a,N)=1$ なる N 以下の素数に対し N が a を底とする Euler 擬似素数 (または強擬似素数) かどうか調べれば良い。つまり (2)(または (3)) が成立するかどうかをみれば良い。a を一つきめて N が (2) (または (3)) を満たすかどうか調べることを Solovay-Strassen テスト ((3) の場合は Miller-Rabin テスト) ということもある。N が素数でないならば、ある a に対し N は a を底とする Euler 擬似素数 (強擬似素数) でない。N が合成数ときこのような a がどの程度あるかは次の命題 7 でわかる。

命題 7 [18, 19].
$N=\prod_{i=1}^{r}p_i^{e_i}$ を N の素因数分解とし、$v_2(a)$ を $a=2^{v_2(a)}a'(a'$は奇数$)$ となる整数とする。更に $\nu_0=v_2(N-1)$, $\nu_i=v_2(p_i-1)$ $(1\leq i\leq r)$, $\nu=\min_{1\leq i\leq r}\nu_i$, $N-1=2^{\nu_0}N'$, $p_i-1=2^{\nu_i}p_i'$ とする。

1. $L_{SS}(N)=\{a\in(\mathbf{Z}/N\mathbf{Z})^*|a^{\frac{N-1}{2}}\equiv(\frac{a}{N})\mathrm{mod}N\}$ とすると

$$\#L_{SS}(N)=\delta_N\prod_{1\leq i\leq r}\left(\frac{N-1}{2},p_i-1\right)$$

但し

$$\delta_N=\begin{cases}2 & \nu=\nu_0,\\ 1/2 & \nu_i<\nu_0(\text{ある奇数の } e_i \text{ の } i \text{ に対して})\\ 1 & \text{その他}\end{cases}$$

2. $L_{MR}(N)=$
$\{a\in(\mathbf{Z}/N\mathbf{Z})^*|a^{N'}\equiv 1\mathrm{mod}N,$ またはある $k(1\leq k<\nu_0)$ に対し $a^{2^kN'}\equiv -1\mathrm{mod}N\}$
とすると

$$\#L_{MR}=\left(1+\frac{2^{r\nu}-1}{2^r-1}\right)\prod_{1\leq i\leq r}(N',p_i')$$

この結果を用いると

系 A

N が合成数ならば

$$\frac{\#L_{SS}}{\varphi(N)} \leq \frac{1}{2}, \qquad \frac{\#L_{MR}}{\varphi(N)} \leq \frac{1}{4}$$

(ただし φ は Euler 関数)

系 B

N が合成数ならば $A_N = \{m : \text{odd} | m \leq N\}$ とすると

$$\lim_{N\to\infty} \frac{1}{\#A_N} \sum_{m\in A_N} \frac{\#L_{MR}(m)}{\#L_{SS}(m)} = \frac{1}{2}$$

が示される。

以上より次のことがわかる。

1. N が合成数のとき N と互いに素な a を random に取ると N が $epsp(a)$ とならない確率は $\frac{1}{2}$ 以上である。
2. N が合成数のとき N と互いに素な a を random に取ると N が $spsp(a)$ とならない確率は $\frac{3}{4}$ 以上である。
3. Miller-Rabin テスト は Solvay-Strassen テスト より倍以上確かである。

先に述べたように、N が合成数ならば a を $2,3,5,\ldots$ と素数を動かしてゆけば N 以下のある値で必ず N は $epsp(a)(spsp(a))$ にならない。つまり以上をまとめると、ある正の整数 c と $\mathbf{Z}_+ \times \mathbf{Z}_+$ から { 合成数、不明 } への多項式時間で計算可能な関数 $\mathcal{F}$ があって

1. 任意の合成数 n に対し
   a.
   $$\mathcal{F}(n,r) = \text{"不明"または"合成数"} \quad for \quad all \quad r$$
   b.
   $$\frac{\#\{r | \log r \leq \log^c n, \mathcal{F}(n,r) = \text{合成数}\}}{\#\{r | \log r \leq \log^c n\}} \geq \frac{1}{2}$$

($\frac{1}{2}$ は Miller-Rabin テストを用いると $\frac{3}{4}$ になる。)

$\mathcal{F}(N,r)$ は N が合成数かどうかを判定する関数で補助数 r (Solovay-Strassen test の a と思って良い) を必要とする。N が素数ならば“不明”になり N が合成数ならば適当な r の集合で半分以上の r に対し“合成数”となる。即ち N が合成数なら確率 $\frac{1}{2}$ 以上で $O(\log^k p)$ (k は p に関係しない定数) の計算量で判定できる。即ち N が合成数ならばその判定は確率的多項式時間問題である。

3. Miller の方法

繰り返してのべるが 命題4 により

Nが合成数ならばある $a(1 \leq a \leq n, (N,a) = 1))$に対し$N$は(2)((3))を満たさない。

Nが素数ならば全ての$a(1 \leq a \leq N, (N,a) = 1)$に対し$N$は(2)((3))を満たす。

故に N の素数判定は $1 \leq a \leq N(N,a) = 1$ なるすべての a に対し Solovay-Strassen テスト (または Miller-Rabin テスト) を行えばよい。しかしこのような a の数は $\varphi(N)$ 個あり、かなり多い。N が素数か合成数 ($epsp(a)$, $spsp(a)$ でない) かを決定するにはどの程度の a まで調べたらよいのかを考えよう。つまり N が合成数のとき N が $epsp(a)$ にならない最少の a を考える。容易に解るように $L_{SS}(N)$ は群である。したがって剰余群 $G_N = (\mathbf{Z}/N\mathbf{Z})^*/L_{SS}(N)$ が定義される。更に N が合成数のとき命題7系 A より G_N は $\{e\}$ でない。したがってこの群のある恒等指標でない Dirichlet 指標 χ と $\chi(a) \neq 1$ となる元 $a \in G_N$ が存在する。このとき N は $epsp(a)$ ではない。この a の値の上からの評価を考えればよいのであるがこれは大変難しい。素数判定を多項式時間内に行えることを保証する評価を得るには、現在のところ一般 Riemann 予想を仮定する必要がある。

一般 Riemann 予想

χ を Dirichlet 指標とすると L- 関数 $L(s,\chi)$ は $Res > \frac{1}{2}$ で零点を持たない。

この予想の仮定の下で

任意の trivial でない N を法とする Dirichlet 指標 χ に対し、ある $a \in \mathbf{Z}, a = O(\log^2 N)$ があって (具体的には $a < 2\log^2 N$) $\chi(a) \neq 1$ となる。

が示される [3]。

G_N の trivial でない指標 χ を考えると、上の結論より N が合成数のとき、ある $a < 2\log^2(N)$ があって $\chi(a) \neq 1$ となる。即ち N が $epsp(a)$ でないということが示される。χ は Dirichlet 指標ということしかわからないが χ を特定することができる。一般 Rieman 予想は非常に難しいので χ を特定しても証明の困難なことは変わりがないと思われる。しかし χ を決めておくことは理論上興味がある。以下の事実により、素数判定に必要な χ は平方剰余記号に限定して良いということが結論される。

定理　8[12].

N を suare free の合成数とする。このとき $p|N$ なる素数 p で $p \equiv 1 \bmod 4$ となるもの、または $p, q|N$ なる素数 $p(\neq)q$ で $pq \equiv 1 \bmod 4$ となるものが存在する。この mod 4 で 1 と合同になる p または pq を d とし $\chi(a) = \left(\frac{a}{d}\right)$ とする。L- 関数 $L(s,\chi)$ が一般 Riemann 予想を満たすとするとある $a < O(\log^2 N)$ があって N は $spsp(a)$ でない。

これらのことより N は Miller 法で $O(\log^5 N)$ の計算量で素数か合成数か判定できる。即ち

一般 Riemann 予想の仮定の下で素数判定は確定的多項式時間問題である。

実験結果 [22] によると $N(< 2 \times 10^{12})$ が合成数のとき、ある $a < 2\log N \log\log N$ ($2\log^2 N$ でない!!) が存在して、N は $spsp(a)$ にならない。

4. 楕円曲線を用いた素数判定法

4.1. Goldwasser-Kilian の方法

整数 a, b に対して素数 p を法とする楕円曲線 $E_p = E_p(a,b)$ とは

$$Y^2 \equiv X^3 + aX + b \mathrm{mod} p$$

の解 $(x \mathrm{mod} p, y \mathrm{mod} p)$ の全体に仮想的な一点 $\mathcal{O}$ を付け加えた集合に次のような演算 $+$ を定義したものである。

2 点 $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$ に対して $P_3 = P_1 + P_2$ の座標 (x_3, y_3) は

$x_1 \not\equiv x_2$ の場合:

$$\lambda \equiv (y_2 - y_1)(x_2 - x_1)^{-1}$$

$x_1 \equiv x_2, y_1 \equiv y_2 \not\equiv 0$ の場合:

$$\lambda \equiv (3x_1^2 + a)(2y_1)^{-1}$$

とし

$$\nu \equiv -\lambda x_1 + y_1$$

とおけば

$$\begin{aligned} x_3 &\equiv \lambda^2 - x_1 - x_2 \\ y_3 &\equiv -\lambda x_3 - \nu \end{aligned}$$

となる。

$x_1 \equiv x_2, y_1 \equiv -y_2$ の場合:

$$P_3 \text{は} \mathcal{O} \text{になる。}$$

ただし計算は全て mod p で行う。つまり $(x_2 - x_1)^{-1}, (2y_1)^{-1}$ は $(x_2 - x_1), (2y_1)^{-1}$ の逆元である。また $\mathcal{O}$ は (x, y) の型には書けなくて、1 変数増やして射影平面で考えると $[0,1,0]$ と書けるものである。この演算 $+$ で E_p は可換群になる。零元は $\mathcal{O}$ である。E_p の位数に関しつぎの Hasse の定理は重要である。

定理　9.(Hasse)

$$p + 1 - 2\sqrt{p} \leq \#E_p \leq p + 1 + \sqrt{p}$$

必ずしも素数と限らない一般の整数 N を法とする楕円曲線の定義はかなり面倒になる。この場合 $P_1 + P_2$ が定義されないこともある。このときも楕円曲線を E_N とかくことにする。

定理　10.(楕円曲線を用いた素数判定法)

N に対しある a, b(ただし $(N, 4a^3 + 27b^2) = 1$) と $\mathcal{O} \neq M \in E_N(a,b)$ と素数 $q > N^{\frac{1}{2}} + 1 + 2N^{\frac{1}{4}}$ があって $qM = \mathcal{O}$ となれば N は素数である。

証明

もし N が合成数ならばある素数 $p < \sqrt{N}$ があって p は N を割り切る。$qM = \mathcal{O}$ を modulo p で考えると $qM_p = \mathcal{O}_p$ となる。即ち M_p の E_p における位数 m_p は q の約数である。故に Hasse の定理を用いると

$$m_p \leq \#E_p \leq p+1+2\sqrt{p} \leq N^{\frac{1}{2}}+1+2N^{\frac{1}{4}} < q$$

となる。q は素数だから $m_p = 1$ となり $M \neq \mathcal{O}$ と矛盾する。
証明終わり

Goldwasser-Kilian[7] の判定法は $\#E_N = 2q(q$は素数で$N^{\frac{1}{2}}+1+N^{\frac{1}{4}}$より大) となる楕円曲線を探して N の素数判定を行う。つまり

(1) a, b を rondom にとる。

(2) Schoof[20] のアルゴリズムにより多項式時間の計算量で $m = \#E_N$ を計算する。

(3) $m = 2 \times q(q > N^{\frac{1}{2}}+1+N^{\frac{1}{4}})$ の型か判定し、なっていなければ (1) からやり直す。

(4) E_N の点 M で条件 $qM = \mathcal{O}$ を満たすものを探す。

(5) q についても同じ方法で素数であることを示す。(再帰)

を実行すする。

4.2. Goldwassr-Kilian 法の計算量

前節で解説した Goldwasser-Kilian の素数判定法の計算量を考える。

定理 11.(Lenstra,Jr.[15])
N を素数とし S を区間 $[N+1-\sqrt{N}, N+1+\sqrt{N}]$ に含まれる整数全体の部分集合とする。このとき

$$\#'\{E_N | \#E_N \in S\} \geq c_1(\#S-2)\sqrt{N}/\log N(c_1 > 0)$$
$$\#'\{(a,x,y) \in (\mathbf{F}_p)^3 | 4a^3+27b^2 \neq 0, \#E_N(a,b) \in S(b = y^2-x^3-ax)\}$$
$$\geq c(\#S-2)p^{5/2}/\log p(c > 0)$$

となる。但し $\#'$ は $\mathbf{F}_p$ 上の同型類の個数である。

Goldwasser-Kilian の方法では楕円曲線の位数 $\#E_N$ が

$$N+1-2\sqrt{N} \leq \#E_N \leq N+1+2\sqrt{N}$$

の範囲でどのくらい $2 \times q$(素数) の形になっているかが問題であった。素数 q は $(N+1-2\sqrt{N})/2 \leq q \leq (N+1+2\sqrt{N})/2$ をみたすが Lenstra,Jr. の定理 11 によりこのような (a,x,y) は $c \times (\#$(S に含まれる素数$)-2)p^{5/2}/\log p$ 個より多い。即ち

$$\frac{\#\{E_N|\#E_N = 2\times q, q\in S, q\text{は素数}\}}{\#\{E_N\}}$$
$$\geq c\times \frac{\pi\left(\frac{N+1+\sqrt{N}}{2}\right)-\pi\left(\frac{N+1-\sqrt{N}}{2}\right)-2}{\sqrt{N}\log N}$$

となる。この分子の $\pi\left(\frac{N+1+\sqrt{N}}{2}\right)-\pi\left(\frac{N+1-\sqrt{N}}{2}\right)-2$ に関し次の Cramer の予想がある。

Cramer の予想

ある正の定数 c_1, c_2 があって十分大きな x に対し

$$\pi(x+\sqrt{x})-\pi(x)\geq c_1\sqrt{p}/\log^{c_2}(x)$$

である。またこの予想の確からしさを支持するものに HeathBrown の定理がある。

定理　12.(HeathBrown[8])

$$\iota(a,b)=\begin{cases}1, & \#\{[a,b]\text{に含まれる素数の個数}\}\leq (b-a)/(2\lfloor\log a\rfloor)\\ 0, & \text{その他}\end{cases}$$

とするとある定数 α あって十分大きな x に対し

$$\sum_{x\leq a\leq 2x}\iota(a,a+\sqrt{a})\leq x^{5/6}\log^{\alpha}x$$

が成立する。

HeathBrown の定理からほとんどすべての素数 N に対し位数が $2\times q$ 型になる楕円曲線が E_N が十分ある。詳しくいうと

$$\frac{\#\{E_N|\#E_N = 2\times q, q\in S, q\text{は素数}\}}{\#\{E_N\}}\geq c\frac{1}{\log^k N}$$

となり定理 10. の条件を満たす E_N (即ち a と $b, \#E_N = 2\times q, q$ は素数で $N^{\frac{1}{2}}+1+N^{\frac{1}{4}}$ より大) が見つかる可能性がある。

多分素数と思われる数 N の素数判定に　$q = \#E_N/2$ が素数判定が必要になるがこの判定は再帰的にこの方法で行う。$q < (N+1+2\sqrt{N})/2$ だから q は N よりかなり小さいので素数判定は N の場合より容易である。N が素数ならば q も素数になりやすいが (Cramer の予想と HeathBrown の定理) 必ずしもそうでない。従って N が素数であることが証明できるにはある意味の"運"がよくないといけない。つまり q が素数となる楕円曲線をうまくとる、さらに q が素数であることを示すのにまた楕円曲線をとる、このとき新たに取った楕円曲線の位数が"運"よく 2 と素数 q' の積になっている必要がある。,q' に関しても同様、...。"運"は Cramer の予想が成立しない部分では全く期待できない。HeathBrown の定理によればこのような部分は密度 0 である。即ち (Cramer の予

想を仮定しなければ)"ほとんど"すべての数 N に対し"運"がよいと (つまり $(1/\log(N)$ の多項式) 以上の確率で) 多項式時間で素数と判定できる。つまり

ほとんどすべての素数判定は確率的多項式時間問題である。

さらに Cramer の予想を仮定すれば"ほとんど"の部分は取れて

素数判定は確率的多項式時間問題である

となる。

4.3. Adelman-Huang の方法

上述のように GoldWaser-Kilian の方法は Cramer の予想 (未解決) を用いる必要がある。この部分を避けるために Adelman-Huang は超楕円曲線を使う素数判定法を考えた [2]。

p を素数とする。

$f \in F_p[x]$ を重根を持たない 6 次多項式とするとき $y^2 = f(x)$ で定義される平面曲線 $C = C(f)$ はいわゆる超楕円曲線である。

$C(f)$ に対応するヤコビ多様体を $J(f)$ とあらわす。$J(f)$ の F_p- 有理点を $J(f)_p, J(f)_p$ の個数を $D(f)_p$ と表す。p が素数でないとき (N と表わす) も $J(f)_N$、$D(f)_N$ が考えられる。

定理　13.

$$n_{\pm}(x) = x^2 \pm 4x^{1.5} + 6x \pm 4x^{0.5} + 1$$

とすると素数 p に対し

$$n_-(p) \leq D(f)_p \leq n_+(p)$$

が成立する。

定理　11 と同様にして次の命題 15 が示される。

命題 14

ある $C(f)$ があって $D(f)_N$ が素数で $M = < a, b > - < a, -b > \in J(f)_N (b^2 = f(a))$ が $D(f)_N M = O$ となるならば N は素数である。

これが Adleman-Huang の algorithm の主要部である。Goldwasser-Kilian 法のときと同様に問題となるのは $D(f)_N$ (=q とする) が素数かどうかの判定である。q は定理 13 により

$$N^2 - 4N^{1.5} + 6N - 4N^{0.5} + 1 \leq q \leq N^2 + 4N^{1.5} + 6N + 4N^{0.5} + 1$$

となるがこれより狭い区間 $[N^2 - N^{1.5}, N^2]$ に素数がたくさんあることが次の定理で保証されている。

定理　15.(Iwaniec-Jutila[9])

ある正の数 d があって十分大きな数 x に対し

$$\pi(x^2) - \pi(x^2 - x^{1.5}) > \frac{x^{1.5}}{\log^d x}$$

である。

残る困難は次の問題である。楕円曲線の場合は $q(=\#E_N)$ が素数かどうか問題になっている数 N の約半分になっているのでより易しい問題にに帰着されている。ところがこの場合は N の素数判定に大きさが約 N^2 の数 $q(=D(f)_N)$ の素数判定が必要になる。この困難を解消するのが次の定理である。

定理 16.

ある正の整数 a_0 があって以下の五つの条件 (1)-(5) を満たす任意の a, p, q に対し

$$\frac{1}{\log^{74} p} \leq \frac{\#\left\{ \begin{array}{r| r} & 0 < g, h < p, 4g^3 + 27h^2 \not\equiv 0, \\ < g, h > \in \mathbf{Z}^2 | & \#E_p(g,h) = lq, l : prime, \\ & \lfloor \frac{a}{q} \rfloor \leq l \leq \lfloor \frac{a}{q} \rfloor + \lfloor \sqrt{\frac{a}{q}} \rfloor \end{array} \right\}}{\#\{ < g, h > | g, h \in \mathbf{Z}, 0 < g, h < p \}}$$

である。

1. $a > a_0$
2. p, q は素数
3. $a \leq p \leq a + \sqrt{a}$
4. $(\pi(\frac{a}{q} + \frac{\sqrt{a}}{q}) - \pi(\frac{a}{q})) > \frac{\sqrt{a}}{10q \log q}$
5. $q \leq (2 \log a)^{70}$

である。簡単にいえば、大きい素数 p (条件 1, 3) と比較的小さい素数 q (条件 5) で $[\frac{a}{q}, \frac{a}{q} + \frac{\sqrt{a}}{q}]$ にはかなりの素数が存在する (条件 4) ものに対し、$\#E_p(g,h) = lq(q$は素数$)$ となる $E_p(g,h)$ は全体の $1/(\log p)^{74}$ より多い。

前述の定理 16 で問題となるのは条件 4. である。このような q がたくさんあるのを保証されている。それを以下で解説する。

定義 17.

i) 1 以上の整数 x が任意の $q < e^{\sqrt{\log x}}$ に対し

$$\pi(\frac{x}{q} + \frac{\sqrt{x}}{q}) - \pi(\frac{x}{q}) > \frac{\sqrt{x}}{10q \log x}$$

となるとき x を full という。

ii) 3 以上の n に対し集合 $P(n), B(n), C(n)$ を次のように定める

$$P(n) = \left\{ (n, q_1, q_2, ..., q_z) \middle| \begin{array}{r} z = \lfloor \log n / (140 \log \log n) \rfloor, \\ 任意の i(1 \leq i \leq z) に対し q_i は素数, \\ 任意の i(1 \leq i \leq z) に対し \frac{(\log n)^{70}}{3} \leq q_i \leq (\log n)^{70}, \\ 任意の i(1 \leq i \leq z-1) に対し q_i < q_{i+1} \end{array} \right\}$$

$$B(n) = \left\{ (n, q_1, q_2, ...q_z) \in P(n) | ある i に対して \lfloor \frac{n}{\prod_{j=1}^{i} q_j} \rfloor は \text{ full でない。} \right\}$$

$$C(n)=\left\{(n,q_1,q_2,...,q_z)\in P(n)|(n,q_1,q_2,\ldots,q_z)\in B(n)\text{又は}\lfloor\frac{n}{\prod_{j=1}^{z}q_j}\rfloor\text{は ample でない}\right\}$$

定義　18.
$3\leq n\in\mathbf{Z}$ に対し

$$\frac{\#B(n)}{\#P(n)}\leq\frac{1}{4}$$

が成立するとき n を ample という。

定義　19.
$3\leq n\in\mathbf{Z}$ に対し

$$\frac{\#C(n)}{\#P(n)}\leq\frac{1}{2}$$

が成立するとき n を very ample という。
これらの定義のもとで以下の命題が成立する。

命題　20.
任意の $\epsilon>0$ に対しある x_0 があって $x>x_0$ ならば

$$\#\{n\in\mathbf{Z}|0\leq n<x,n\text{は}full\text{でない}\}<x^{\frac{5}{6}+\epsilon}$$

命題　21.
$0\leq x\in\mathbf{Z}$ とし

$$\epsilon_1(x)=\{n\in\mathbf{Z}|0\leq n\leq x,n\text{は}ample\text{でない}\}$$

とするとある $c<\frac{15}{16}$ があって十分大きな x に対し

$$\#\epsilon_1(x)<x^c$$

命題　22.
十分大きな数 n_0 に対し $n>n_0$ のとき n が ample ならば n は very ample である。
これらの事実と定理 10.,11.,12. を用いて Adelman-Huang は次の定理を示した。

定理　23.(一般化された Goldwasser-Kilian の定理)
ある 0 以上の整数 β と正の数 $c<\frac{15}{16}$ と多項式時間で計算できる $\mathbf{Z}_+^2$ から { 合成数、不明 } への関数 $\mathcal{H}$ があって次の条件を満たす。

1. 任意の合成数 n に対し $\mathcal{H}(n,r)=$ 素数、合成数、不明　for all 正の整数 r
2. 素数 p に対し

$$\alpha_p=\frac{\#\{r\in\mathbf{Z}_+|\log r\leq\log^\beta p,\mathcal{H}(p,r)=\text{素数}\}}{\#\{r\in\mathbf{Z}_+|\log r\leq\log^\beta p\}}$$

とし

$$\epsilon(x) = \{p : prime | p \leq x, \alpha_p < \frac{1}{2}\}$$

とすると

$$\#\epsilon(x)(\leq \#\epsilon_1(x)) < x^c$$

となる。($\epsilon(x) \subset \epsilon_1(x)$ であることに注意)

また Adleman-Huang[2] は次の定理を示した。

定理　24.

$$S = \{(n, f) \in \mathbf{Z}_+ \times (\mathbf{Z}/n\mathbf{Z})[x] | \deg f = 6\}$$

とする。ある正の整数 α と多項式時間で計算できる $\mathbf{Z}_+^2$ から $\mathbf{Z}$ への関数 $\mathcal{G}$ があって

1. 任意の $(n, f) \in S$(n は素数、 f は多重根を持たない) に対し
   a.
   $$\mathcal{G}(n, r) = 0 \quad or \quad D(f)_n \quad \text{for all} \quad r \in \mathbf{Z}$$
   b.
   $$\frac{\#\{r \in \mathbf{Z}_+ | \log r \leq \log^\alpha p, \mathcal{G}((n, f), r) = D(f)_n\}}{\{r \in \mathbf{Z}_+ | \log r \leq log^\alpha p\}} \geq \frac{1}{2}$$
2. 任意の (n, f)(f は多重根をもつ) に対し
   $$\mathcal{G}((n, f), r) = 0 \quad \text{for all} \quad r \in \mathbf{Z}$$
3. 任意の $(n, f) \in S$(n は合成数) に対し $\mathcal{G}((n, f), r)$ はすべての $r \in \mathbf{Z}$ で素数でない。

これは楕円曲線の位数を多項式時間で計算する Schoof の algorithmsc 超楕円曲線版と思ってよい。さらに Adeleman-Huang は次の定理も示した。この定理のの証明は Adleman-Huang[2] の約 2/3 を費やすもので超楕円曲線で位数が素数になるものが十分たくさん存在することの証明である。

定理　25.

素数 p, q に対し $N(p, q) = \#\{f \in F_p[x] | f$は多重根をもたない。$D(f)_p = q\}$ と定めると二つの正の整数 d, e が存在して

$$\frac{\#\left\{q \middle| \begin{array}{c} p : \text{prime} p^2 - p^{1.5} \leq q \leq p^2 \\ N(p, q) < \frac{p^{5.5}}{\log^e(p)} \end{array}\right\}}{\#\{q | q : \text{prme}, p^2 - p^{1.5} \leq q \leq p^2\}} \geq \frac{1}{\log^d(p)}$$

これら定理 23,24,25 を用いるとつぎのことがいえる。

ある正の整数 c と多項式時間で計算される $\mathbf{Z}_+^2$ から {素数、合成数、不明} への関数 $\mathcal{F}$ があって

1. 任意の合成数 n に対し $\mathcal{F}(n,r)$ = 合成数、不明 for all $r \in \mathbf{Z} \quad (0 \leq r)$

2. 任意の素数 p に対し

$$\frac{\#\{r|\log r \leq log^c p, \mathcal{F}(p,r) = \text{素数}\}}{\#\{r|\log r \leq log^c p\}} \geq \frac{1}{2}$$

これが Adleman-Huang[2] の結論である。
さて証明であるが次の定理 26 からすぐ解る。

定理 26.
ある正の整数 t と $g \in \mathbf{Z}[x]$ と多項式時間で計算される $\mathbf{Z}_+^2$ から{素数、合成数、不明} への関数 $\mathcal{F}$ があって

1. 任意の合成数 n に対し

$$\mathcal{F}(n,r) = \text{合成数、不明} \quad for \quad all \quad r$$

2. 任意の素数 p に対し

$$\frac{\#\{r|\log r \leq g(\log p), \mathcal{F}(p,r) = \text{素数}\}}{\#\{r|\log r \leq g(\log p)\}} \geq \frac{1}{\log^t(p)}$$

この定理 26 の証明の outline を示そう (かなりの省略があるので詳しくは Adleman-Huang を参照のこと)。

$$S(p) = \{q \in [p^2 - p^{1.5}, p^2] | q : prime, N(p,q) > p^{5.5}/\log^e p\}$$

とし (定理 25 参照)

$$U(p) = \{(p, q_1, q_2, q_3) | q_1 \in S(p), q_2 \in S(q_1), q_3 \in S(q_2)\}$$

$$T(p) = \{(p, q_1, q_2, q_3) \in U(p) | q_3 \notin \epsilon(p^8)\}$$

とする (定理 23 参照)。このとき

$$\#T(p) \geq \frac{p^{5.5}}{\log^{c_1} p}$$

何故なら $V(q) = \{(p, q_1, q_2, q_3) \in U(p)\}$ とすると

$$\#T(p) \geq \#U(p) - \sum_{q \in \epsilon(p^8)} \#V(q)$$

定理 15, 25 より

$$\#U(p) \geq p^{1.5} p^3 p^6 / \log^{c_2} p = p^{10.5} / \log^{c_2} p$$

更に $(p,q_1,q_2,q_3)\in V(q)$ だから

$$q^{1/2}\leq q_2\leq q^{1/2}+q^{1/4}, q_2^{1/2}\leq q_1\leq q_2^{1/2}+q_2^{1/4}$$

従って $q\in\epsilon(p^8)$ に対し $\#V(q)\leq pp^2=p^3$ 一方定理25によりある $c_3(<7.5)$ があって $\#\epsilon(p^8)\leq p^{c_3}$ となる。故に $\#\epsilon(p^8)\#V(q)<p^{3+c_3}(3+c_3<10.5)$ となり、十分大きな素数 p に対し $\#T(p)\geq p^{10.5}/\log^{c_4}p$ が成立する。
また $(p,q_1,q_2,q_3)\in T(p)$ に対し

$$K((p,q_1,q_2,q_3))=\{(h_0,h_1,h_3)|h_0\in F_p[x],D(h_0)=q_1,h_i\in F_{q_i}[x],D(h_i)=q_{i+1}(i=1,2)\}$$

$$W(p)=\cup K((p,q_1,q_2,q_3))$$

とおくと定理15,23により

$$\#K((p,q_1,q_2,q_3))>p^{38.5}/\log^{c_5}(p)\quad(38.5=10.5+4+8+16)$$

$$\#W((p,q_1,q_2,q_3))>p^{49}/\log^{c_5}(p)\quad(49=10.5+38.5)$$

となる。$\mathcal{F}$ を定理23の $\mathcal{H}$ を用いて

$$\mathcal{F}(n,r)=1-\prod_{i=0}^{z}(1-\mathcal{F}'(n,r_i)))$$

r_i,z は n,r より決まる数 $\mathcal{F}'$ は n に対し $q_1\in S(n),q_2\in S(q_1),q_3\in S(q_2)$ とすると $\mathcal{F}'(n,r)=\mathcal{H}(q_3,r)$。この評価を用いれば $g(x)=49x+(1+2^\alpha+4^\alpha)x^\alpha+8^\beta x^\beta\in F[x]$ とおくと

$$\#\{r|\quad|r|\leq g(|p|)\}\leq c_6p^{49}d$$

$$\#\{r|\quad|r|\leq g(|p|),\mathcal{F}(p,r)=1\}\geq p^{49}d/\log^{c_6}(p)$$

(ただし $d=\#\{r|\quad|r|(1+2^\alpha+4^\alpha)p^\alpha+8^\beta p^\beta$ である) が示される。これで定理26が示された。

algorithm を簡単にのべる。ほとんど確実に素数である自然数 N の素数判定をしたい。

(1) mod N 超楕円曲線を定義する六次式を random にとり、その Jacobi 多様体の位数 q_1 を計算する。(定理 24.) これが素数であることが示されれば N の素数判定ができる。

(2) q_1 の素数判定にまた mod q_1 の超楕円曲線をランダムにとってその Jacobi 多様体の位数 q_2 を計算する。q_2 の素数判定ができればよい。

(3) この判定に三度 mod q_2 の超楕円曲線をランダムにとってその Jacobi 多様体の位数 q_3 を計算する。q_3 は約 N^8 の大きさである。

(4) q_3 の素数判定には定理 10. を用いる。すなわ mod q_3 の楕円曲線を random にとり、その位数 m_1 が小さい確定素数 p_1 と (判定が必要な) 素数 ℓ_1 の積になることを示す。この ell_1 の素数判定に再び定理 10. の方法を使う。つまり mod Ell_1 の楕円曲線を random にとり、その位数 m_2 が小さい確定素数 p_2 と (判定が必要な) 素数 ℓ_2 の積になることを示す。以下同様に再帰的に $ell_i(1 \leq i)$ の素数判定を行い N が素数であることを示す。

何故 (4) でつぎつぎに ell_i がすべて素数になりやすいかは定理 23. による。定理 26. の証明のなかで示したように q_3 はほとんど $\epsilon(p^8)$ の元にならない (定理 23. による)。即ち q_3 は ample と思ってよい。ample の定義 18. と定理 17. から ℓ_1 は素数になりやすい。さらに命題 22. により $\lfloor q_3/\prod_{i=1}^{z} q_i \rfloor$ がまた ample なので同じことが更に繰り返され、ほとんどの場合 ell_i がすべて素数となる。

以上のことにより Adleman-Huang の方法で

全ての素数 p は確率的多項式時間で素数と判定できる

ことが示された。

参 考 文 献

[1] Adleman, L. M., Pomerance, C. and Rumely, R. S., *On distinguish prime numbers from composite numbers*, Ann. of Math. 117(1983), 173–206.

[2] Adleman, L. M. and Huang, M. A., *Primality testing and abelian varieties over finite fields*, Springer Lecture Notes in Math. 1512(1992).

[3] Ankey, N. C. *The least quadratic non-residue* Annals of Math. 55(1952),65–72

[4] Bosma, W. and van der Hulst M.-P., *Primality proving with cyclotomy*, Doctorial Thesis, University of Amsterdam, 1990.

[5] Cohen, H. and Lenstra, Jr., H. W., *Primality testing and Jacobi sums*, Math. Comp. 42(1984), 297–330.

[6] Cohen, H. and Lenstra, A. K., *Implementation of a new primality test*, Math. Comp. 48(1987), 103–121.

[7] Goldwasser, S. and Kilian, J., *Almost all primes can be quickly certified*, Proc. 18th annual ACM symp. on Theory of Computing(1986), 316–329.

[8] Heath-Brown, D. R., *The Differences between consecutive primes*, J. London Math. Soc. 18(1978), 7–13.

[9] Iwaniec, H. and Jutila, M., *Primes in short intervals*, Ark. Mat. 17(1979), 167–176.

[10] Knuth, D. E., *The art of computer programming, vol 2, Seminumerical algorithms*, Addison-Wesley 1973

[11] Lenstra Jr., H. W. *Miller's primarity test*, Inform. Process. Lett. 8-2(1979) 86–88

[12] Lenstra Jr., H. W., *Primality testing algorithms*, Springer Lecture Notes in Math. 901(1981), 243–257.

[13] Lenstra Jr., H. W., *Galois theory and primality testing*, Springer Lecture Notes in Math. 1142(1985), 169–189.

[14] Lenstra Jr., H. W., *Divisors in residue classes*, Math. Comp. 42(1984), 331–334.

[15] Lenstra Jr., H. W., *Factoring integers with elliptic curves*, Ann. of Math. 126(1987), 649–673.

[16] Miller, G. L., *Riemann's hypothesis and tests for primality*, J. Comp. and System Sc. 13(1976), 300–317.

[17] Morain, F., *Courbes elliptiques et tests de primalité*, Docteure Thèse, L'Université Claude Bernard-Lyon I, 1990.

[18] Monier, L., *Evaluation and comparison of two efficient prbabilistic primarity algorithms*, Theoret. Comput. Sci. 12(1980), 97–108

[19] Rabin, M. O., *Probabilistic algorithm for testing primarity* J. Number Theory 12(1980), 128–138

[20] Schoof, R., *Elliptic curves over finite fields and the computation of square roots mod p*, Math. Comp. 43(1985), 483–494.

[21] Solovay, R and Strassen, V., *A fast Monte-Carlo test for primarity*, SIAM J. Comput. 6–1(1977), 84–85 7–1(1978),118

[22] Wagon, S., *Primarity testing* Math. Intellgencer 8–3(1986), 58–61